The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

Paper No. 25

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JOHN PHILIP PETTITT

Appeal No. 2005-0099
Application No. 09/442,106

ON BRIEF

Before KRASS, BLANKENSHIP, and SAADAT, Administrative Patent Judges.

BLANKENSHIP, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134 from the examiner's final rejection of claims 17-30, which are all the claims remaining in the application.

We reverse.

BACKGROUND

The invention relates to detecting fraud in credit card transactions when ordering and downloading information over the Internet. Claim 17 is reproduced below.

> 17. A method for detecting fraud in a transaction between a consumer and a merchant over the Internet, wherein the transaction involves the consumer purchasing a product from the merchant using a credit card, the method comprising the steps of:
>
> receiving, from the merchant, transaction information that identifies the consumer and the product, including an Internet address of the consumer;
>
> receiving, from the merchant, credit card information associated with the consumer that identifies the credit card to be used in the transaction;
>
> verifying the credit card information based upon a consistency check that determines whether the credit card information matches the consumer;
>
> verifying the credit card information based upon a history check that determines whether the credit card information is consistent with the transaction information;
>
> verifying the credit card information based upon an automatic verification system;
>
> verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other transactions that are associated with the Internet address of the consumer;
>
> creating and storing a fraud score value based on the verifying steps that provides the merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

The examiner relies on the following references:

Gopinathan et al. (Gopinathan)	5,819,226	Oct. 6, 1998

Wallace	5,988,497	Nov. 23, 1999 (filed May 30, 1996)

Philip McCrea et al. (McCrea), "The Internet Report," Australian Taxation Office Electronic Commerce Project, 184 pages (Jun. 1997).

Robert Richardson (Richardson), "Neural Networks Compared to Statistical Techniques," Computational Intelligence for Financial Engineering, Proceedings of the IEEE/IAFE 1997, pp. 89-95 (Mar. 1997).

Claims 17-26 and 28-30 stand rejected under 35 U.S.C. § 103 as being unpatentable over Wallace, McCrea, and Gopinathan.

Claim 27 stands rejected under 35 U.S.C. § 103 as being unpatentable over Wallace, McCrea, Gopinathan, and Richardson.

An earlier rejection of the claims under the judicially created doctrine of obviousness-type double patenting has been withdrawn by the examiner.

We refer to the Final Rejection (Paper No. 15) and the Examiner's Answer (Paper No. 18) for a statement of the examiner's position and to the Brief (Paper No. 17) and the Reply Brief (Paper No. 22) for appellant's position with respect to the claims which stand rejected.

OPINION

The statement of the rejection (Answer at 5-6) contends that Wallace teaches detecting fraud in a transaction involving the purchase of a product between a consumer and a merchant over the Internet. As later elaborated upon in the Answer, Wallace discloses that a "second tier of validation" may be required for transactions relating to geographical limitations (col. 2, ll. 4-10). Specifically, in the context of bank cards, the card holder could specify a geographical condition, such as the second tier of validation should be initiated only if an ATM machine outside a predetermined set of ATM machines is used. Col. 4, ll. 13-17.

The examiner finds that Wallace fails to teach the use of an Internet address in the detection of fraud in a credit card transaction by verifying if the information about physical addresses associated with the Internet addresses used in the transactions are consistent. However, the rejection asserts that McCrea teaches the use of Internet addresses in verifying the physical address associated with the Internet address, relying in particular on material at pages 95 through 96, 112, and 159 through 161 of the reference. It would have been obvious, according to the rationale of the rejection, to modify Wallace to use Internet addresses in detecting credit card fraud by verifying information about the physical address associated with the Internet address used in the transaction.

Appellant submits, inter alia, that McCrea is a report prepared for the Australian Taxation Office. Appellant argues that McCrea provides no teaching or suggestion of linking an Internet address with a physical address, beyond determining whether the Internet address is associated with subnets in Australia. (Brief at 6-7.)

McCrea teaches (at 93-94) that each computer has a unique IP number (or "address") which describes the topological location of the computer. The IP address comprises a network part which identifies a subnet and a host part that identifies a computer on the subnet. A computer may be on more than one subnet, in which case the computer will have multiple IP addresses. An IP packet, containing data to be transferred on the Internet, contains a source and a destination IP number.

McCrea further teaches (at 95-97) that IP addresses are the primary way of identifying computers engaged in Internet activities. By combining the address with information in routers it is possible to find out exactly where a subnet is located. Finding which IP addresses are in Australia, which is important in identifying commercial Internet activity in Australia, may be achieved in steps that include finding all IP links into Australia. McCrea further notes, however, that one IP packet may be encapsulated within another IP packet (by a process known as "tunnelling"), with the result that the inner IP packet might travel by a route different from that which would have been chosen for it by the intervening routers. As a result, "tunnels" make it possible for computers to have IP addresses that are not formally assigned to the physical location of the computer.

Further, McCrea teaches (at 112) that location may be ascertained from link layer information, "and perhaps indirectly identity...." Ascertaining location "may be appropriate for criminal investigation but would not normally be feasible for the higher volume investigations of tax compliance." Id.

McCrea also notes (at 161) that although each Internet-enabled computer has a unique IP address, the address may be assigned temporarily to a computer by the Internet access provider while the computer is connected to the Internet, and then reassigned to a different computer during a different session. Consequently, there is not necessarily a correlation between an IP address and the geographical location of a computer. Id.

Finally, we note that pages 159 through 160 of the reference, upon which the rejection relies, deal with collecting information from a "Webshop" (i.e., a merchant's web site) relating to that web site's address, rather than information concerning a consumer's transaction.

In view of the foregoing teachings of McCrea, when read in context of the reference, we are in ultimate agreement with appellant. All of the claims on appeal contain limitations similar to those of representative claim 17, which requires that transaction information be collected, "including an Internet address of the consumer," and "verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other transactions that are associated with the Internet address of the consumer...." We find no motivation from the prior art for applying the teachings of McCrea regarding Internet addresses to those of Wallace in order to enhance the Wallace system (i.e., to enhance determination whether a "second tier of validation" in a transaction is indicated). As such, the proposed combination of Wallace and McCrea could only arise from an improper hindsight reconstruction of the invention. The other references (Gopinathan and Richardson) applied against the claims do not remedy the basic deficiency in the rejection.

The arguments presented in § 11 of the Answer are not persuasive, particularly those alleging what may be "analogous," "inherent," or "obvious." The Answer does not establish a foundation for the respective position by pointing out objective teachings in evidence provided in support of the rejection. The allocation of burdens requires that the USPTO produce the factual basis for its rejection of an application under 35 U.S.C. § § 102 and 103. In re Piasecki, 745 F.2d 1468, 1472, 223 USPQ 785, 788 (Fed. Cir. 1984) (citing In re Warner, 379 F.2d 1011, 1016, 154 USPQ 173, 177 (CCPA 1967)).

We thus do not sustain the rejection of claims 17-26 and 28-30 under 35 U.S.C. § 103 as being unpatentable over Wallace, McCrea, and Gopinathan, nor the rejection of claim 27 under 35 U.S.C. § 103 as being unpatentable over Wallace, McCrea, Gopinathan, and Richardson.

CONCLUSION

The rejection of claims 17-30 under 35 U.S.C. § 103 is reversed.

REVERSED

ERROL A. KRASS)
Administrative Patent Judge)
)
)
Howard B. Blankenship)
) BOARD OF PATENT
HOWARD B. BLANKENSHIP) APPEALS
Administrative Patent Judge) AND
) INTERFERENCES
)
Mahshid D. Saadat)
)
MAHSHID D. SAADAT)
Administrative Patent Judge)

HBB/dpv

HICKMAN PALERMO TRUONG & BECKER LLP
1600 WILLOW STREET
SAN JOSE , CA 95125-5106